NETWORK SECURITY AND FORENSICS

Prof. OBADIAH OGHOERORE ALEGBE PhD

Electronics Engineer

Professor of Computer Engineering Universidad Nacional de Tres de Febrero Buenos Aires Argentina

Professor of Information Engineering Universidad de Belgrano Buenos Aires Argentina

Professor Collegium Ovirium Buenos Aires Argentina

Table of Contents:

1. Introduction.

2. ISO/OSI and IP protocol attacks.

3. Reference Models.

4. Authentication.

5. Types of Firewall, Intrusion Prevention and Denial of Service.

6. Secure Network Devices, Embedded Systems Security

7. Network Traffic Analysis, Packet capture and analysis, Wireless security.

8. Conclusion.

Chapter 1.

Introduction.

In this write-up, we shall analyze Computer Networks Security and its Forensics. As the Information Highway lifts mankind higher and higher in space, so also the concerns of Business, Governments, Institutions, Corporations are increased as regards security and it has become a priority.

Professionals in Networking and Forensics now focus hardily against non-authorized access and intrusion to computer networks. They focus attention on hacking, identity theft, industrial espionage, and government espionage, all which have produced awareness on the risks to confidential information.

It must be borne in mind that for information to be secured over the internet, it must be available, it must possess integrity and it must be confidential. Likewise those accessing such information must be authenticated, authorized no repudiating.

Insecure networks can corrupt Information and when information is corrupt it becomes inaccessible and thus it loses integrity. So in the case we have unauthorized modification made on information by human errors o noise on commination media or any other source.

Some dangers could be the erasure of datum from computers (data loss) for this reason when the data is needed, it is not available.

In many cases during electronic fund transfer and financial accounting, data can be tampered with. In Air Traffic control error in data being processed can lead to disasters.

In all time, users of the internet want to be sure that:

- The information on hand is trustworthy.
- When they share information, it must be in a responsible way.
- The information must always be available.
- They must have a system that will process the information in a trustworthy and timely manner.

The four points raised are very useful to the user but none of the points are elements for forensics but they are to Network Administrators because they are no crime.

Access and Intrusion are trespasses of high degree and thus crime, these then give work to forensics.

Access and Intrusion are not always a crime unless Justice declares it so, the forensic can only limit to verify that there was access or intrusion and if possible by who.

The paragraph above just gave us the link between Network Security and Forensics. Network Security, the first depends on the Network Administrator while verification of security breach depends on the forensic proxied through Justice.

We shall here go through Networking threats which forensics can verify.

Chapter 2.

ISO/OSI and IP protocol attacks.

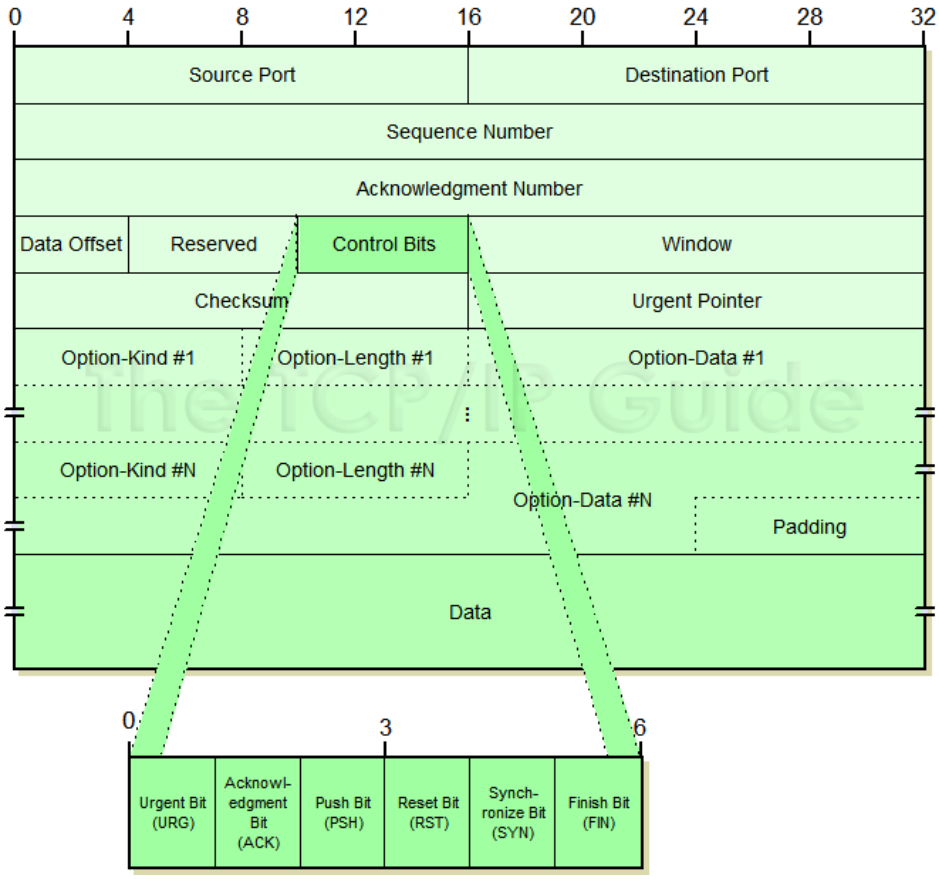
TCP/IP Transmission Control Protocol/Internet Protocol was created to make sure that all communications can survive under any condition without affecting the integrity of data even under malicious attacks.

OSI Open System Interconnection Basic Reference Model was developed to standardize networking and it is an abstract description of protocol for networks.

The TCP/IP end point first establish connection prior to transmission. Within this protocol are data units called segments. So transmitting and receiving data with this protocol are done in segment form made or fixed 20-byte header and a sizable data field.

Through TCP, TCP breaks bytes of data stream into segments and reconnecting them together at the receiving end where it recognizing them in the correct order. In case of data loss, the protocol allows retransmission of data loss.

The Segment format of TCP



The source port and destination ports identify the endpoints of the transmission. Every port combined with its IP Address form a unique endpoint.

The Sequence Number and Acknowledgement Number contain the number of bytes in the stream

Data offset is also known as TCP header length which indicates how man words (4-byte) are contained in the TCP header.

The Window field tells about how many bytes of data can be transmitted before acknowledgement is received.

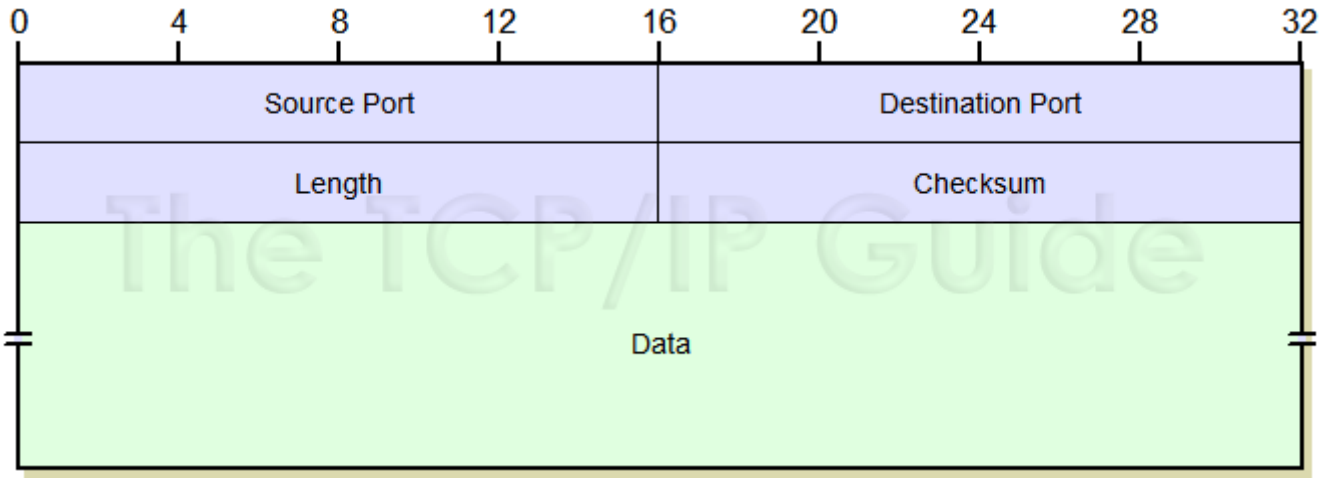
The checksum provide the reliability and security of the TCP segment.

The user data is placed at the end of the header.

UDP User Datagram Protocol is of lesser fields compared to TCP. Real time traffic are transported efficiently without the need for error correction and thus no retransmission necessary.

UDP is a protocol without connection and its reliability depends on the application layer. It is about fast transmission.

The Segment format of UDP



The type of transport protocol to use depends on the data type to transfer. If Reliability sf important, then TCP is recommended.

Attack:

As we can see in the block diagrams, the standards are set and every bit through the networks has an identity and its purpose. Software is responsible for collecting data and composing all according to protocol and sending it through the ports where all are converted into trains of electronic bits through the networks.

So also software can be developed to compose attack codes which are put into protocol and transmitted through the networks. The crime comes in when software simulates the foreign machine IP and uses it to send data to the remote networks. All these are very possible.

The good news is that though the source and remote IP can be simulated, the routes cannot be easily simulated, this fact becomes helpful to forensics to identify the source and route of attack because as data travels various communication equipment especially router record the presence of data through them and forensic experts can now trace the route to crime source.

Chapter 3.

Reference Models.

In understanding the Concept of Network Security, two types of networks can be devised. These are:

a. Unified Network. This type of Network, the Network System and the collection of IS are accredited as a single entry. Its properties include:

- The architecture and Design of its security must be readily understandable.
- Its representation must be of single security domain.
- Only one single authority must administer it.
- All its hardware, software and devices must have well defined parameters around it.
- All its boundaries including users must be well understandable.

- It must possess a mode of operation that is overall.

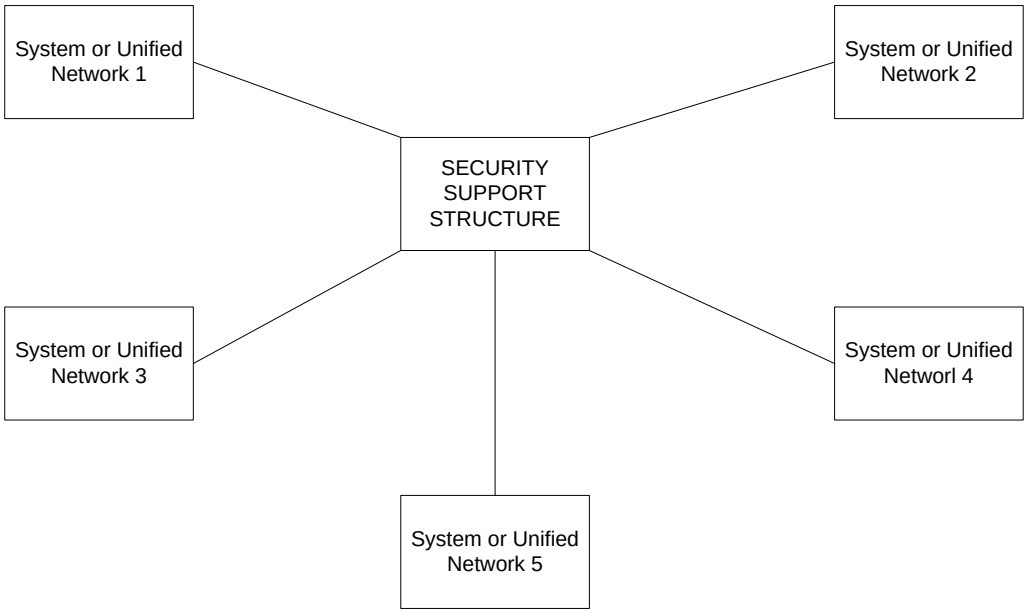
b. Interconnected Networks: In this case it is composed of separately accredited IS or Unified Networks. This type of network must have Identifiable Security Support Structure (ISSS). This ISSS must be able to adjudicate different security policies of each participating IS or Unified Networks. This kind of network needs accreditation even as simple as Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA). The Properties of such network include:

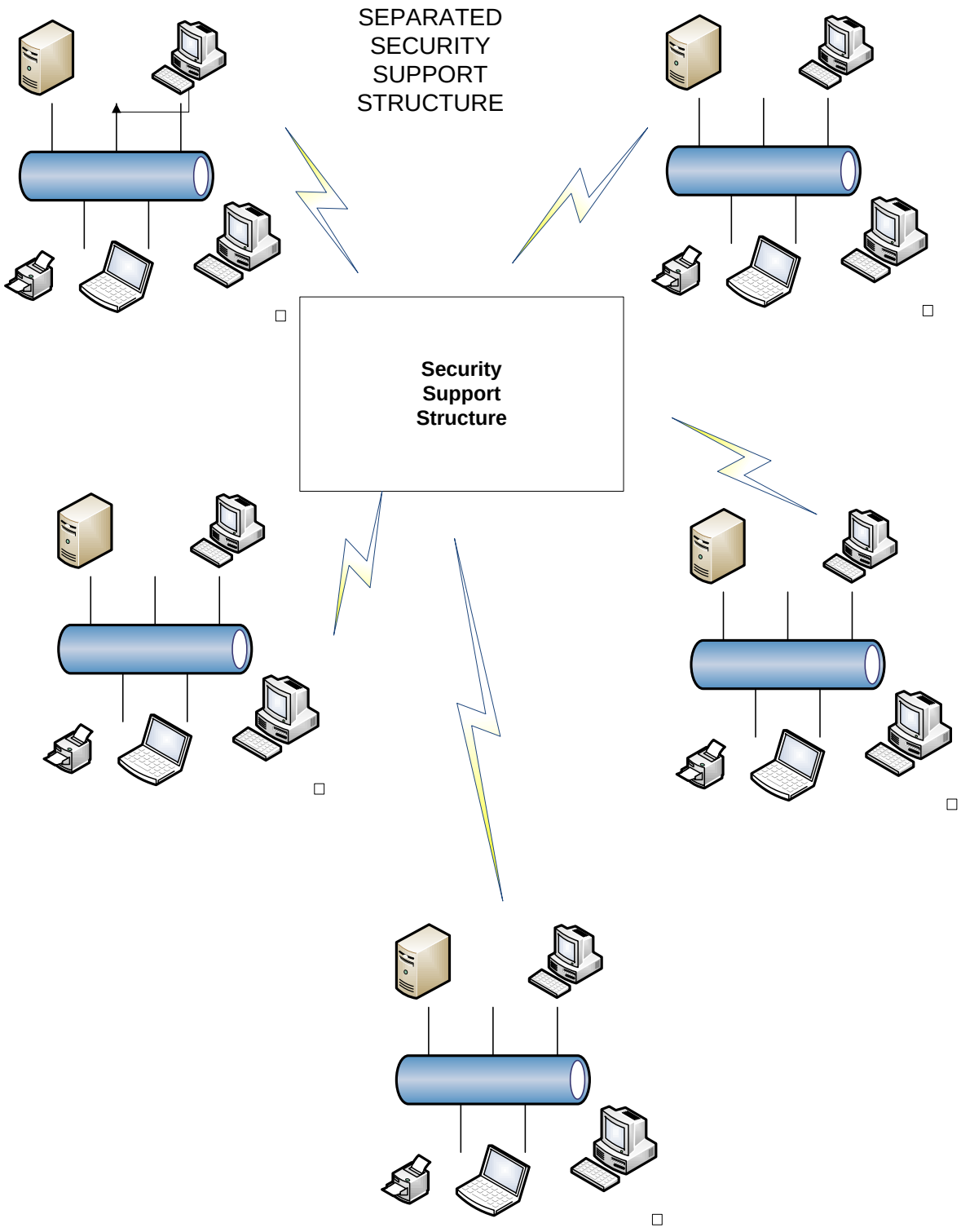
    1. The Security Across the whole Interconnected Networks must have an understandable approach. It will be best if there is a MOU/MOA between all those responsible for the security of each member Network.

    2. The interconnection of Network has two basic approaches, which are **Directly Connected** and **Indirectly Connected**.

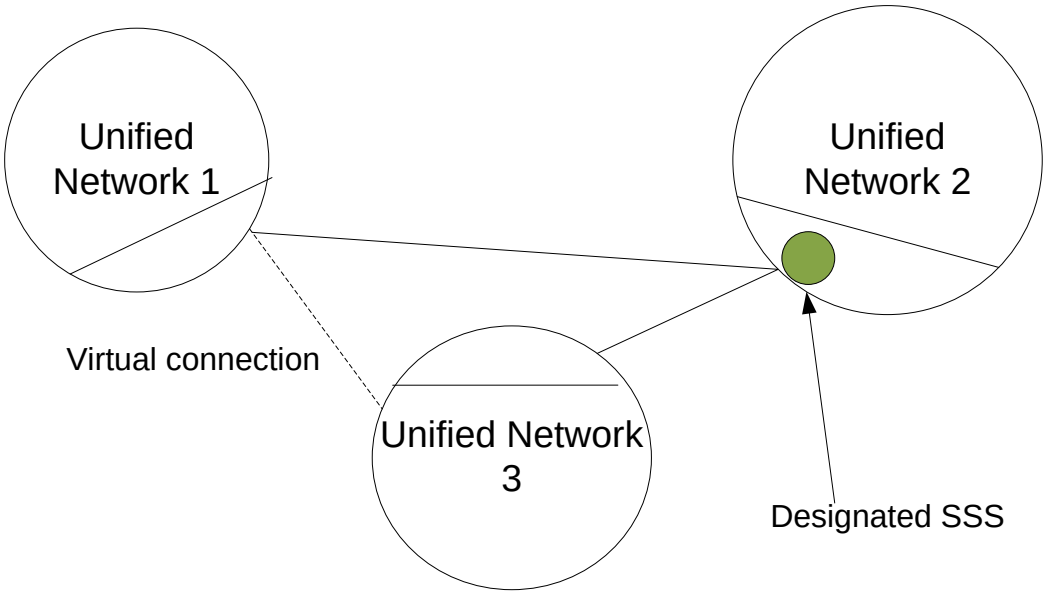
        a. Directly Connected have three basic Architectural Choices for the SSS that is needed to adjudicate security policy and differences implementation between or among them:

            i. Hardware, software y firmware may be differently identifiable in SSS whose aim is to provide secured inter-connection of the contributing systems. It thus forms a gateway between all of them that any two that communicates must pass through this gateway and the gateway asks for passports and “visa” before allowing any communications through.


System or Unified Network 1
System or Unified Network 2
SECURITY SUPPORT STRUCTURE
System or Unified Network 3
System or Unified Networl 4
System or Unified Network 5

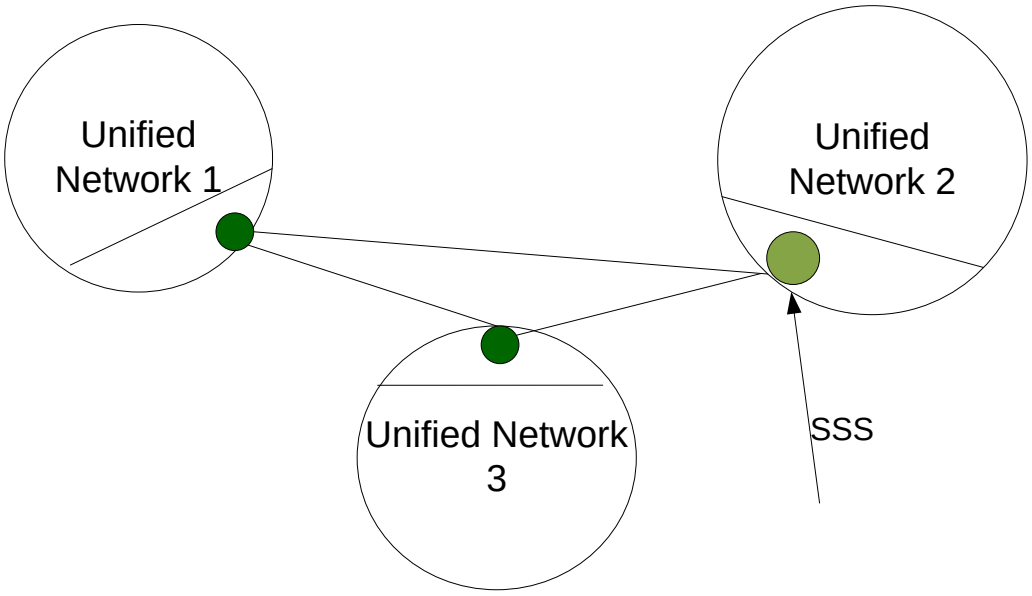


ii. The SSS may be provided by one the many members as shown below.

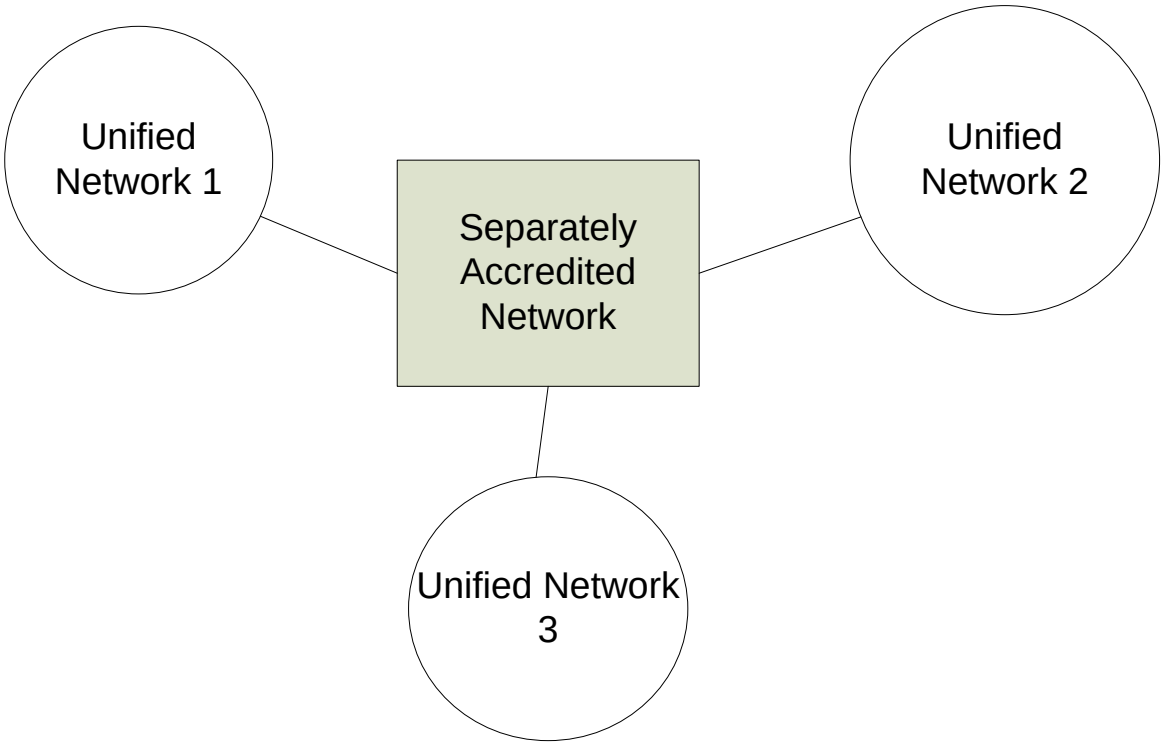


It can be observed in the diagram that Networks 1 and 3 connect through the Designates SSS installed in Network 2 that also share the same SSS with the rest.

iii. In this case each Network has its own SSS and thus the SSS is distributed as shown below.



iv. In this case, there is an intermediate Network that manages the accreditation.



The simple description above is just to show ways of modeling networks to facilitate the administration of the security system. Such modeling also helps Forensic Expert during their search for evidence about Network Crimes.

Chapter 4.

Authentication.

Authentication is the process of confirming that a data is true. In this case data could be anything given like documents or anything whose identification needs confirmation.

In Networking, it is used to control access to network or parts of the network. There are many hardware like routers and communications equipments that contain security control by which access can be allowed o restricted to certain computers identifiable by MAC o IP and Users. During communication, router checks for the identity of user before acting as programmed to do. There is also another authentication on webpages where users need to enter their user name and passwords for authentication before being allowed in. This is used in webmail's and even all mail clients have to access mail servers with user name and password.

The following are examples of Authentication methods which also are helpful in forensics.

Password: With this method, the user will input and identifier which is usually a typed text along with another representing a password which are authenticated in the corresponding server for approval. This method has many vulnerabilities because it can be guessed and it can be discovered by eavesdropping.

One-time password: One time password allows it to be used only once after which it expires.

Public-key Cryptography: It is based on mathematical algorithm that uses two keys, one public and the other private. These two keys are related through very complex mathematical algorithm and equation. The private key is employed to decrypt and encrypt messages between computing machines. A public key is used to encrypt and verify signatures.

Zero-knowledge proofs: In this method a Host is convinced by another to allow access without revealing any secret data. Here a client create a random problem which is very difficult to solve after which it solves the problem with the information it has. After solving, it commits a solution through bit-commitment scheme after which it sends the commitment and problem to the server. The server will then ask the client to prove that the problems are related. This goes through various steps and algorithm before access is granted.

This method has its own share of problems because while the Host A thinks that it is showing the proof of its identity, Host B can simultaneously authenticate a third party Host C by using the credentials of Host A.

Widely used Authentication Protocols:

1. **Secure Sockets Layer:** Secure Sockets Layer is a secure method provided TCP the connection communications. It is also used for HTTP Connections. Here both server and client send greetings (usually) to each other with which the established connection. After the greetings, the sever sends certificate for authentication. After this encrypted data follow until the process of authentication complete.

2. **IP.SEC:** The header of the authentication of the IP provides a very powerful authentication and integrity for the datagram of the IP. It uses different algorithm. The authentication is protocol independent. The data of the authentication is calculated with an algorithm of message digest.

3. **Secure Shell:** SSH is a protocol that is used to provide secure remote login and it is also used over insecure network to provide secure network services.

4. **Keberos:** This method developed by MIT has two main components. These are a ticket that is used for authentication and for securing data and an Authenticator which is used to verify that the user is the one to which the ticket was originally granted. During the login, there is connection from the system to the Keberos server from where it retrieves a session key which will be used between the user and the ticket granting service. Its is encrypted based on user password. If the client introduced the right password the system at the end will be able to decrypt the password. After completion of the authenticated process, the password is erased from the memory to prevent compromising the system.

To conclude, the authentication method to be used depends on the usability. The factor of usability can be ignored during the design of authentication system. If the method of authentication used is not usable by the users forced to use them, they will tend to ignore the system or bypass them. It is very important to bear in mind Usability when adopting and maintaining security system.

Chapter 5.

Types of Firewall:

The growth of the Information Highway has brought about the need for security awareness. Firewall plays important part in this security for the networks. For us to understand a bit more about firewalls, we will briefly mention about data packets.

A data packet contains three headers and application data:

a) Network Header.

b) Transport Header.

c) Application Header.

Network Header	Transport Header	Application Header	Application Data

The headers correspond to three well known layers Network Layer, Transport Layer and Application Layer.

The Application layer is consisted of several protocols like File Transfer Protocol (ftp) , Hyper Text Transfer Protocol (http) and Simple Mail Transfer Protocol (SMTP).

Transport Layer consists of TCP, UDP.

Network Layer consists of IP.

A Firewall can be defined as a system of both hardware and software projected and installed to provide security for an Information Network. For this, all traffic into and out from the Network must pass through the Firewall.

The types of Firewall mostly in use are as follows:

1. **Packet Filter:** A set of rules are set usually for access control in a list, this filter evaluates all packets that it receives according to the rules set. The rules may be source and destination IPs that are allowed in specific lapse of time and the type of protocol allowed through the network.
2. **Application Gateway Firewalls:** In this case the Firewall acts as a proxy, it accepts connection from a side and checks if it is permitted, if so it makes the connection to the other side. Here there is control as which application

running inside the network can communicate outside the computer or network.

3. **Socks:** Socks was designed for TCP-based client server application. The Socks Proxy pass only traffic that are related to Socks so that its client software must process all traffic through the proxy that is recognized.

4. **Stateful Inspection:** There is a technique that provides best security to Networks with fast performance. It is called Stateful Multi-Layer Inspection (SMLI). It makes security tighter while at the same time making it easier and less expensive to use. This type has the advantage that it closes all TCP ports and then dynamically opens them when required.

5. **Hybrid Firewalls:** Virtual Private Network. This incorporates end-to-end encryption into the network, and then enables a very secure connection to be established between an individual computer and a protected network.

Firewall to be used depends of the philosophy of design and then the appropriate product can be selected.

Intrusion Prevention: A primitive approach to the security of networks that leads to the detection of threats and provide swift response is called Intrusion Prevention. Intrusion Prevention constantly is at alert to identify potential threats and to move swiftly into responding to the threaat. For this to happen, it monitors the network traffic.

There are cases where attackers gain access to networks, in which case Intrusion prevention has the ability to act immediately based on some set of rules. This could be done by blocking ports that are not allowed for communications. Intrusion Prevention System when they detect packets suspected to be threats possibly because it goes through unauthorized ports can raise alarm and also drop the suspected data packets.

There are different kinds of Intrusion preventions and could be arranged into four or more classes:

1. **Intrusion Prevention Systems that are Network-Based**. These permanently are monitoring the networks in search of suspicious traffic. This is done through the analysis of Protocol Activities.

2. **Intrusion Prevention System for Wireless Networks**: These systems monitor all wireless networks for any suspicious packets. They do it by analyzing network protocol in wireless communications.

3. **Analysis of Network behavior**: In this case the network traffic is examined to identify threats that can produce or generate unusual flow of traffic. The check whether there is violation of policy by some form of malware and distributed denial of service.

4. **Intrusion Prevention System based on Host Machines or Systems**: In this case there is software installed in the Host Machine which monitors for suspicious activities. This is done by analyzing the vents that occur within the host.

These Intrusion Prevention Systems employ among other three basic methods which are:

- Detection based on Signature.
- Detection based on anomaly in Statistics.
- Detection based on the analysis of Stateful Protocol.

Denial of Service Attack:

This is also called Distributed Denial of Service (DDoS) Attacks. This is an attempt to make a network users access to some resources from some machines.

The goal of this attack to block or interrupt connection of computers to the internet. There are bots today that sent DoS attack to hosts and networks. They usually attack banks and Credit Car companies. They attack websites. They can get installed in a computer in a network from where they send out packets to saturate the networks.

The United States Computer Emergency Readiness Team has given ideas about how to detect the presence of Denial of Service Attack and they include:

- Network Performance is very slow especially during opening of files and accessing websites.
- Some particular websites may not be available.

- Some websites may not be accessible.
- The number of spams emails received is dramatically increased. This kind is called a-mail bomb.
- Frequent disconnection of wired and wireless network connection.
- Denial of web access during a long time by computers from a network.

The methods they use in attacks include:

- Consumption of all resources of a computer.
- Disconfiguration of information for example of routing in computers.
- It can reset TCP sessions to prevent the computer form communication effectively.
- Physical Network components disruption.
- Obstruction of communication between users and victims to prevent flowing communications.

Chapter 6:

Secure Network Devices:

There are electronic devices used to secure networks. Depending on the network is the sophistication of the devices.

The first basic device is the computer itself running operating systems. The Operating systems can be configured to open or block communications port inside TCP. The operating system can be configured to allow certain programs to run or not. Linux is an operating system that by default will not allow most programs to run except with permission.

Windows now come with firewall that is configurable to allow certain programs to run or not. So in home based computers or network with few computers, it is just enough to configure the operating system in each computer.

In case of larger Networks, two devices that provide security are Routers and Firewall. They come in hardware and software.

Many routers have firewall built inside them for network administrators to configure.

Firewall monitors the traffic between the Network and the Internet, when it detects unusual traffic, it suspects that there is a computer in the network that is compromised, it blocks the traffic and in some cases sends email to the administrators.

In case of Wireless Routers, they come with security system that is encrypted. So that with an encrypted password, the router allows connections. Two basic Encryption types are Wireless Encryption(WEP) or Wi.fi Protected Access (WPA).

Embedded System Security:

Embedded devices are of the order of the day. The technological revolution produced by micro-electronics has boosted embedded device. Embedded devices are usually handheld devices that run operating system of different kinds. This devices are computer based that is they contain micro-computers like those within the structure of desktop computers. Already we have multicore processors in embedded system that runs on Windows and Android. This means that some software running on windows can run in embedded system, analogically threats to computers are also threats to embedded systems.

Since most embedded devices transfer data through the internet, they too are not immune from attacks. For this reason, these devices need to be secured.

Embedded devices thus also need user and password to protect its data. It can be noted that banking, business transaction are now done over the internet from handheld devices like mobile phones and Tablets, the danger is posed as with all networks.

For this reason protocol are setup for embedded devises in order to safe data to and from them. We can classify Security needs for embedded system into two basic types:

- Data Transfer Security Needs.
- Internal Security Needs within the device.

In the first case, baring in mind that data is transferred through many unsafe and untrustworthy communication media, it is very important that data from and to embedded system be encrypted. We have already explained Data Encryption. Apart from Data Encryption, when there are many embedded devices involved there is need for Public-Key Agreement Algorithm in the encryption. There is also a need for Digital Signature which also must be encrypted. Digital Signature also must be accompanied by a Digital Certificate.

In the second case that has to do with the internal security needs in the device, the Key Algorithm must be negotiated between devices and there is usual a secret key involved which are stored in each device.

There is a Secure SoC which gives physical protection to all the secrete keys and stores them in a Secure ROM that handles the secrete keys within Soc. The secret keys are encrypted and stores inside the ROM.

Embedded Devices also have Secure-Boot-Loader Signing. Here the secrete key protected by hardware are exposable to some APIs for use. To reduce risks, firmware are designed so that an unauthorized user running some APIs cannot modify its content. During booting, the Secure Boot loader tests if the firmware is genuine, if not it prevents it from booting up the device. Secure boot loader resides in a much protected area of the ROM.

Chapter 7.

Network Traffic Analysis.

As the title says, it is the analysis of all the traffic through a computer network. This is the key to the detection of threat to the security of Computer Networks. All data through networks whether encrypted or not are trains of bits organized through protocol. Protocol makes it possible to tap into the networks and analyze the contents of data flow. The process of analysis is not by blocking but rather by cloning data flow and working on the copy.

The analysis of Data depends on the context that could be military, counter-intelligence and pattern-of-life-analysis. The analysis of traffic may be based on software program running on computers many of which are commercially available.

In Military intelligence, signal intelligence is the main focus to monitor enemy communications and decode them. This even include following if there is communications or not, the length of time of communication and the data transmitted within the communications. This is very possible because all communications equipments are built following protocols even though the data is encrypted. The first step is to separate data from communication before proceeding to cracking into the data no matter the language written into it. Military Intelligence expert take over form there.

Some commercial products of data analysis are the followings:

- Visual Analytics.
- Orion Scientific.
- Pacific Northwest Maritime Labs.
- Genesis EW’s GenCom Suite.
- SynerScope.

There are other Network Traffic Analysis that generates reports on bandwidth and users. These equipments and software offer detailed reports on Applications, users and conversation generating traffic. This equipment also generates graphic reports that are useful in understanding and troubleshooting network traffic.

Some are in software form installed in computer. One suc program is NetFlow Analyzer of Cisco. Since Cisco manufactures communications equipments, it has all the protocols on communications and it is in position to produce software for Network Analysis.

Packet Capture and Analysis.

Communications are done in packets.

What is a Network Packet? It is a unit of data that is formatted according to a norm and carried by packet-switched network. It is consisted of control information and a useful data. Packet-Switched network are network that move data about in small packets.

Let us view the case of email. E-mail messages are broken into some sizes in bytes by the Network. These little pieces are packets. Each packet contains all the information that will lead it to the destination. These information are IP Address of the Sender, IP Address of the remote Receiver, data about the number of packets the e-mail message is broken into, and the index of this current packet. Packets are sent using Transmission Control Protocol/Internet Protocol. Thus each packet is just a part of the message.

The packets are sent though the best available route and the Network administers the efficiency of transmission.

A simple graphical explanation of TCP/IP 32 bit packet is shown below:

IP Header:

<table>
<tr><td>Version</td><td>Length</td><td>Type of Service</td><td colspan="2">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td>Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">Source Address</td></tr>
<tr><td colspan="5">Destination Address</td></tr>
<tr><td colspan="5">Option</td></tr>
<tr><td colspan="5">Data</td></tr>
</table>

TCP

<table>
<tr><td>Source Port</td><td>Destination Port</td></tr>
<tr><td colspan="2">Sequence Number</td></tr>
</table>

Acknowledgement			
Offset	*Reserved*	*TCP Flags* *C E U A P R S F*	*Window*
Checksum			*Urgent Pointer*
TCP Option			

Packets are also called Datagram the basic characteristics are as follow:

- All data transmitted over the internet are in small size called packets. This is usually done in TCP.
- The size of the packet is usually small and data sent out are broken into small packets which at the receiving end put all together.
- Data transmitted over the network are examined by router and switches which in turn direct it to destination.
- When a packet is not received because there is no receipt acknowledgment, it is sent again.

The interception of Data Packets that is transmitted across a Network is called Packet Capture. The captured packet is stored in a data storage for posterior analysis.

Through the analysis of the packet, we can diagnose and solve network problems. It can also be useful to detect security threat which in turn will help create a better set of security policies.

There are different capturing techniques for the analysis of real-time capture. One if its type is Filtering by which filters are connected to Network nodes where data are captured.

There is also a form of capturing whole packets for full analysis.

In all there are software developed to do all necessary analysis of the captured data. These software are able to extract all data from the packets for viewing.

The application and use of packet capturing include:

- For Security Reason: It helps to identify security flaws and breaches and the point where intrusion can take place.

- Identification of Leakage of Data: It will help identify leakage points.
- Troubleshooting: It will help inform about occurrences of events that can compromise the network.
- Identification of Data Loss: it will help identify if data or packets are lost on the way through the network.
- Forensics: Here Administrators can identify the extent of damages done by virus or intruders.

Wireless Security:

Wireless Security prevents Access that is not authorized to and from computers connected via Wireless Networks.

There are two basic and commonly used types:

WEP Wired Equivalent Privacy.

WPA Wi-Fi Protected Access.

Of the two mentioned WEP is very standard because the password can easily be cracked with a basic laptop computer.

WPA is a stronger security which has been replacing WP since 2003. WPA is being upgraded and there is even WPA2 that for some computers to access it, the firmware must be updated.

The disadvantage of wireless networks is that Hackers can through it access networks to do great damages. For this reason, there is need for companies to define effective wireless security policies to block against any unauthorized access to their networks. Examples of these policies are Wireless Intrusion Prevention Systems (WIPS) and Wireless Intrusion Detection Systems (WIDS).

Chapter 8.

Conclusion.

Networking is possible because there is Protocol. Communications between computers is no more direct but through many connectivities which means that every bit transmitted out of any device is passed through all communications devices.

All Communications devices have access to every data through them, they know the origin and the destination, they are able to block or allow data through each of them.

Based on this, no communication is absolutely confidential and there is a degree of insecurity in Networking.

This easy brief of protocol of communications and its possible attack and then unto the ways of securing Networks through authentication, firewall, Intrusion Prevention and Denial of Service.

We also present here some Secured Network Devices and Embedded Security Systems.

The existence of equipment for the analysis of Traffic and Packet Capture provide Forensic Scientists tools which permit them to detect events that the Judiciary can declare as Cybercrime or not.

These devices are able to store information about all the traffic that pass through into a log file that can be studied by Forensics. The difficult task facing Forensic Scientists will be the degree of trust in these devices. Forensics must make sure that Communications Equipment do not alter data for any reason for example, a power failure during traffic and writing into a log file can damage the file. And they must be able to proof that even though there was a power failure, the evidence on hand is reliable.

Even though there are degrees of insecurity in Networks and unreliability in data, het Computer Forensic Experts can still perform their duty to a very high degree of reliability.

References:

Bhagchandka Dhiraj Classification of Firewalls and proxies (2003)

Retrieved From ftp://ftp.cs.utexas.edu/pub/techreports/tr03-28.pdf .

Buchanan William J. Introduction to Security and Network Forensics.

Cecil Alisha –a summary of Network Traffic Monitoring and Analysis Techniques. Retrieved from http://www.cse.wustl.edu/~jain/cse567-06/ftp/net_monitoring.pdf .

Denial of Service Attacks . Types of attacks Retrieved from http://www-rp.lip6.fr/~blegrand/cours/MIAIF/secu1.pdf .

ISO/OSI Model SSL: Security at Transport Layer (2003) Retrieved from http://www.sis.pitt.edu/jjoshi/IS2935/Lecture9.pdf .

McClure Stuart(2009) Hacking Exposed.

Miller Alexander, Schorcht Gunar Embedded Systems Secuirty: Perfomance Investigation of Various Cryptography Techniques in Embedded Systems. Retrieved from http://www.kaspersky.com/images/miller,_alexander_-_embedded_systems_security_performance_investigation_of_various_cryptographic_techniques_in_embedded_systems.pdf .

Sanders Chris (2011) Practical Packet Analysis .

Scarfone Karen, Mell Peter(2007) Guide to Intrusion Detection and Prevention Systems Retrieved from http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf .

Strassberg Keith E. Network Device Security retrieved from

http://media.techtarget.com/searchNetworking/downloads/Network_Device_Security.pdf .

The OSI Refference Model. Retrieved from

http://billatnapier.com/cisco_presentation/osi31.pdf .

Venkataram Prof. Pallapa Network Reference Model Retrieved from http://pet.ece.iisc.ernet.in/course/E2223/ch2.pdf

Wireless Networking Security. Retreived from

http://www.infosec.gov.hk/english/technical/files/wireless.pdf